

HIPAA & RESEARCH



What is Covered under the Privacy Rule?

Protected Health Information (PHI)

- Health information + Identifier = PHI
- Transmitted or maintained in any form (paper, electronic, forms, web-based, etc.)
- Decedents' information included

Does not include de-identified health information.

Covered Entity & Researcher Relationship

Covered Entities = (1) Health Plans, (2) Health Care Clearing Houses, & (3) Health Care Providers who electronically transmit any health information

- Researchers are covered entities if they are also Health Care Providers who electronically transmit health information
- Any entity that meets the definition of a covered entity is generally, in its entirety, subject to the Privacy Rule
- A single entity may elect hybrid status if it performs both covered & non-covered functions

Exceptions to HIPAA TPO

- **Treatment, Payment, Health Care Operations (**TPO**)
 - **Treatment** – the provision, coordination, or management of health care and related services by one or more health care provider, (i.e., consultation, referrals)
 - **Payment** – activities of a health care provider to obtain reimbursement for the provision of health care (i.e., eligibility, coverage, billing, claims management, collections)
 - **Health Care Operations** – such activities as quality assessment and improvement, reviewing qualification of employees and students, medical/legal/compliance reviews, cost-management, internal grievances, customer service, education**

What Research is Affected?

- Records research that uses existing PHI, such as:
 - Research databases and repositories
 - Chart reviews
- Research that includes treatment of research participants, such as:
 - Clinical trials

Research Use and Disclosure of PHI Without Authorization: De-Identified Health Information

- Completely de-identified information (18 elements removed) and no knowledge that remaining information can identify the individual
- De-identified is NOT the same as anonymous!
- Statistically “de-identified” information where a statistician certifies that there is a “very small” risk that the information could be used to identify the individual

What is an Identifier under the Privacy Rule?

The Privacy Rule defines 18 identifiers

- **Name**
- **Geographic information (including city, state and zip)**
- **Elements of dates (including admission/discharge dates; service dates; birth date, date of death)**
- **Telephone numbers**
- **FAX numbers**
- **E-mail addresses**
- **Social Security number**
- **Medical Record number prescription number, etc.**
- **Health plan beneficiary number**
- **Account Numbers**
- **Certification numbers**
- **VIN and Serial numbers, license plate numbers**
- **Device identifiers and serial numbers**
- **Web URLs**
- **IP address numbers**
- **Biometric identifiers (finger prints, voice prints, retinal scans, etc.)**
- **Full face or comparable photo images**
- **Unique identifying numbers**

Research under HIPAA

- Situations in which PHI may be used for research purposes:
 - By De-Identification of PHI
 - With individual Authorization
 - With waiver of Authorization by IRB or Privacy Board
 - As a Limited Data Set with Data Use Agreement
 - As an activity preparatory to research
 - For research on decedent's information

Elements of an Authorization

Core HIPAA Elements

- Description of PHI to be used or disclosed
- Person(s) authorized to make and receive requested use or disclosure
- Purpose for the use or disclosure
- Expiration date or event (e.g. end of the research study or none)
- Subject or legally authorized representative signature and date

Required HIPAA Statements

- Right to revoke Authorization plus exceptions and process
- Ability/Inability to condition treatment, payment, or enrollment/eligibility for benefits on Authorization
- PHI may no longer be protected by Privacy Rule once it is disclosed by the covered entity

Common Rule vs. Privacy Rule

Research WITH subject permission

Common Rule/FDA

Regulated



IRB review of research
and informed consent

Privacy Rule



Valid authorization

Use and Disclosure of PHI for Research *Without* Individual Authorization:

Four Options:

- **Option 1:** Obtain documentation that an IRB or Privacy Board has approved an alteration to or waiver of authorization based on the following 3 waiver criteria:
 1. The use or disclosure involves no more than minimal risk because of an adequate plan/assurance
 - To protect PHI from improper use or disclosure
 - To destroy identifiers at earliest opportunity
 - That PHI will not be inappropriately reused or disclosed
 2. The research could not practicably be conducted without the waiver
 3. The research could not practicably be conducted without access to and use of PHI

Waiver of Authorization

HIPAA

Waiver of requirement for Authorization to use or disclose PHI

- No more than minimal risk to privacy based on at least:
 - Plan to protect identifiers
 - Plan to destroy identifiers at earliest opportunity
 - Written assurance that PHI will not be used/disclosed with few exceptions
- Research cannot be done without waiver
- Research cannot be done without the PHI

OHRP

Waiver of requirement for informed consent

- Research involves no more than minimal risk – the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests
- Waiver or alteration of informed consent will not adversely affect the rights and welfare of the subject
- The research could not be practicably carried out without the waiver
- Whenever appropriate, subjects will be given additional information after participation

FDA

- No comparable waiver of informed consent allowed

Research Use and Disclosure of PHI *Without* Individual Authorization:

- **OPTION 2:** Obtain representation that the use or disclosure is necessary to prepare a research protocol or for similar purposes preparatory to research:
 1. Researcher must provide representation that:
 - The PHI is to be used solely to prepare a protocol or for a similar purpose
 - The PHI will not be removed from the covered entity
 - The PHI is necessary for research
 2. May be used to develop hypothesis, protocol or characteristics of research cohort
 3. May not be summarized, used or presented as a research study without prior IRB approval
 4. May allow access to PHI to identify subjects for recruitment

Privacy Rule and Research: Subject Recruitment

- A patient's direct treatment provider may discuss possible research participation with a patient
- A patient's direct treatment provider may NOT discuss the patient with research colleagues for potential enrollment purposes without the patient's Authorization or Waiver of Authorization by IRB or Privacy Board
- Can a researcher search through medical records to identify potential research subjects?
Only if:
 - They are the subject's direct treatment provider
 - Individual Authorization has been provided
 - A Waiver of Authorization has been granted by the IRB or Privacy Board
 - As Preparatory to Research
- All subject recruitment strategies and material MUST be approved by the IRB (Common Rule requirement)

Research Use and Disclosure of PHI *Without* Individual Authorization:

- **OPTION 3:** Obtain representation that the use or disclosure is solely for research on decedents' protected health information:
 1. The researcher must provide representation that:
 - The use and disclosure is solely for research
 - The PHI is necessary for research
 - The individual is deceased, and provide documentation upon request

Research Use and Disclosure of PHI *Without* Individual Authorization

OPTION 4: Only use or disclose limited data set/"Indirect Identifiers" (e.g. zip code, age, elements of date)

Limited Use Data Set

Excludes the following direct identifiers:

- **Name**
- **Geographic information (other than city, state and zip)**
- **Telephone numbers**
- **FAX numbers**
- **E-mail addresses**
- **Social Security number**
- **Medical Record number, prescription number, etc.**
- **Health plan beneficiary number**
- **Account Numbers**
- **Certification numbers**
- **VIN and Serial numbers license plate numbers**
- **Device identifiers and serial numbers**
- **Web URLs**
- **IP address numbers**
- **Biometric identifiers (finger prints, voice prints, retinal scans, etc.)**
- **Full face or comparable photo images**
- **Unique identifying numbers**

Data Use Agreement REQUIRED for Limited Use Data Sets

The Data Use Agreement must:

- Describe the permitted uses and disclosures (recipient cannot use or disclose PHI in a way that the covered entity cannot)
- Identify who can use and disclose the PHI
- Require the recipient to:
 - Not re-identify the information or contact the individuals
 - Use or disclose information for specified purposes only
 - Apply safeguards to protect the information
 - Report known violations to the covered entity
 - Hold subcontractors to the same standards as in the agreement

Disclosure to a Public Health Authority or Required by Law

- Disclosure without Authorization permitted if required by law or for public health activities
 - Adverse event reporting to a sponsor, FDA, NIH
 - Public health reporting of communicable diseases
 - Tracking of FDA regulated products (e.g. devices)
 - Reporting abuse, neglect or domestic violence
- A covered entity may disclose PHI related to an adverse event if required to do so by regulation. Even if not required to do so, the researcher may disclose adverse events to a public health authority.

State Law

- The Federal Regulations defer to State and Local regulations for definition of the following terms:
 - Legally Authorized Representative (LAR) – surrogate decision maker for subject who lacks capacity.
 - Child – person who has not attained the legal age of consent to research treatments or procedures under applicable state law
 - Guardian – individual authorized to consent to a child’s general medical care under applicable state or local law.
- State law may impose additional obligations that impact research, e.g.:
 - Mandatory reporting (child abuse, communicable disease testing)
 - Additional subject protections (ESBOR)

IRB Member Conflict of Interest

- OHRP and FDA Regulations provide that no IRB member may participate in the review of any project in which the member has a conflicting interest, except to provide information requested by the IRB.
- An IRB may lose its quorum if the number of members falls below a majority when a member with a conflict of interest leaves the room for deliberation and voting on a study.